TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 13 juin 2001 (13.06.01)	
Demande internationale no PCT/FR00/02058	**Référence du dossier du déposant ou du mandataire** PCT76.0591
Date du dépôt international (jour/mois/année) 17 juillet 2000 (17.07.00)	**Date de priorité** (jour/mois/année) 22 juillet 1999 (22.07.99)
Déposant LEYDIER, Robert	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

14 février 2001 (14.02.01)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI **34, chemin des Colombettes** **1211 Genève 20, Suisse**	Fonctionnaire autorisé Diana Nissen

Copie à l'intention de l'office élu (EO/US) PCT/FR00/02058

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et instruction administrative 422 du PCT)

Destinataire:

DEN BRABER, Gérard
Schlumberger Systèmes
Test & Transactions - Propriété Intellectuelle
50, avenue Jean Jaurès
Boîte postale 620 12
F-92542 Montrouge
FRANCE

Date d'expédition (jour/mois/année)
13 juin 2001 (13.06.01)

Référence du dossier du déposant ou du mandataire
PCT76.0591

NOTIFICATION IMPORTANTE

Demande internationale no
PCT/FR00/02058

Date du dépôt international (jour/mois/année)
17 juillet 2000 (17.07.00)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

☐ le déposant ☐ l'inventeur ☒ le mandataire ☐ le représentant commun

Nom et adresse

UTZMANN-NORTH, Anne
Schlumberger Systèmes
50, avenue Jean Jaurès
Boîte postale 620 12
F-92542 Montrouge
FRANCE

Nationalité (nom de l'Etat):

Domicile (nom de l'Etat):

no de téléphone
01.47.46.72.14

no de télécopieur
01.47.46.63.02

no de téléimprimeur

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

☒ la personne ☐ le nom ☐ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse

DEN BRABER, Gérard
Schlumberger Systèmes
Test & Transactions - Propriété Intellectuelle
50, avenue Jean Jaurès
Boîte postale 620 12
F-92542 Montrouge
FRANCE

Nationalité (nom de l'Etat):

Domicile (nom de l'Etat):

no de téléphone
01.47.46.63.72

no de télécopieur
01.47.46.63.09

no de téléimprimeur

3. Observations complémentaires, le cas échéant:
La nomination du mandataire a été révoquée. Un nouveau mandataire a été nommé comme indiqué dans le cadre 2. Un pouvoir signé par LEYDIER, Robert est requis.

4. Une copie de cette notification a été envoyée:

☒ à l'office récepteur
☐ à l'administration chargée de la recherche internationale
☒ à l'administration chargée de l'examen préliminaire international
☐ aux offices désignés concernés
☒ aux offices élus concernés
☐ autre destinataire:

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

Fonctionnaire autorisé:
Diana Nissen

02

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
PCT76.0591		
Demande internationale n°	Date du dépôt international *(jour/mois/année)*	(Date de priorité (la plus ancienne) *(jour/mois/année)*
PCT/FR 00/ 02058	17/07/2000	22/07/1999
Déposant		
SCHLUMBERGER SYSTEMES		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

   a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

   [ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

   b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

   [ ] contenu dans la demande internationale, sous forme écrite.

   [ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

   [ ] remis ultérieurement à l'administration, sous forme écrite.

   [ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   [ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   [ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

   [X] le texte est approuvé tel qu'il a été remis par le déposant.

   [ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

   [ ] le texte est approuvé tel qu'il a été remis par le déposant

   [X] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 5

   [X] suggérée par le déposant.

   [ ] parce que le déposant n'a pas suggéré de figure.

   [ ] parce que cette figure caractérise mieux l'invention.

   [ ] Aucune des figures n'est à publier.

Cadre III TEXTE DE L'ABREGE (suite du point 5 de la première feuille)

L'invention concerne un micro-contrôleur (30) destiné à être incorporé dans un objet portatif du type carte à puce, comprenant au moins:
- un plot (VCC) pour l'alimentation en courant dudit micro-contrôleur (30);
- un plot (I/O) d'entrée et/ou de sortie de données;
- une partie efficace de traitement de données (°CE); et
- des informations confidentielles.
Selon l'invention, le micro-contrôleur comprend en outre: - des moyens (GEN, CAP, COM) pour faire varier la tension d'alimentation de la partie efficace de traitement des données (°CE), lesdits moyens étant aptes à sécuriser lesdites données confidentielles contre des attaques en courant.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 00/02058

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		DE 68900160 D	29-08-1991
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
US 4827451 A	02-05-1989	FR 2604554 A	01-04-1988
		DE 3766351 D	03-01-1991
		EP 0269468 A	01-06-1988
		JP 63106852 A	11-05-1988
EP 0108011 A	09-05-1984	FR 2535488 A	04-05-1984
		DE 3370217 D	16-04-1987

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
CT/FR 00/02058

A. CLASSEMENT DE L'OBJET DE L[illegible]NDE
CIB 7 G06K19/073

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06K G11C G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 juin 1990 (1990-06-05) le document en entier	1
A	US 4 827 451 A (FRUHAUF SERGE ET AL) 2 mai 1989 (1989-05-02) colonne 4, ligne 18 -colonne 6, ligne 64; figures 2,4	1
A	EP 0 108 011 A (THOMSON CSF) 9 mai 1984 (1984-05-09) page 2, ligne 20-34; figures 1,4,5	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
3 novembre 2000	10/11/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cardigos dos Reis, F

1

INTERNATIONAL SEARCH REPORT

Interna tal Application No
PCT/FR 00/02058

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G11C G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990 (1990-06-05) the whole document	1
A	US 4 827 451 A (FRUHAUF SERGE ET AL) 2 May 1989 (1989-05-02) column 4, line 18 -column 6, line 64; figures 2,4	1
A	EP 0 108 011 A (THOMSON CSF) 9 May 1984 (1984-05-09) page 2, line 20-34; figures 1,4,5	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 November 2000	10/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cardigos dos Reis, F

Form PCT/ISA/210 (second sheet) (July 1992)

10/031681

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 76.0591	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR00/02058	International filing date (*day/month/year*) 17 July 2000 (17.07.00)	Priority date (*day/month/year*) 22 July 1999 (22.07.99)
International Patent Classification (IPC) or national classification and IPC G06K 19/073		
Applicant SCHLUMBERGER SYSTEMES		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 14 February 2001 (14.02.01)	Date of completion of this report 07 September 2001 (07.09.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR00/02058

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1, 2, 4, 5, 7-18, as originally filed,
pages _____, filed with the demand,
pages 3, 3a, 6, filed with the letter of 11 July 2001 (11.07.2001),
pages _____, filed with the letter of _____.

☒ the claims, Nos. 8-12, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-7, filed with the letter of 11 July 2001 (11.07.2001),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1-8, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-7	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-7	NO
Industrial applicability (IA)	Claims	1-7	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following documents:

D1: US-A-4 932 053

D2: US-A-4 827 451.

1. The present invention **relates** to a microcontroller designed to be added to a smart card, for example. The integrated circuit comprises two active portions: a microcontroller interface portion (µCl in Figure 5) and an effective data processing portion (µCE with CPU, RAM EEPROM, ROM, etc.).

The **problem** addressed by the present invention can be considered that of securing such a microcontroller against "attacks based on current consumption" (an attack which aims to obtain confidential data controlled by the microcontroller, for examples keys, by displaying the time-based I_{cc} current of the microcontroller by means of a computer connected to a digital oscilloscope, in order to sample and digitize the results obtained with a view to a non-real time analysis). The **solution** proposed in the invention is a means for varying the supply voltage to the effective data processing portion (µCE). This variation

(preferably random) of the voltage disturbs the electric signals and makes it difficult or even impossible to analyze them. The energy consumed by the microcontroller therefore does not reveal the instructions executed by the microcontroller and, hence, the confidential data implemented in the execution of said instructions. It is no longer possible to obtain confidential information by analyzing the I_{cc} current.

2. **Document** D1 relates to the same problem as the application (see abstract, column 1, lines 40-45 and column 2, lines 29-46). This document, which is the closest prior art, describes a microcontroller designed to be added to a smart card (column 1, line 13), including:
- a contact pad for the power supply to said microcontroller (column 3, line 29: V_{cc})
- a contact pad for inputting and outputting data (column 1, line 22)
- an effective data processing portion (column 1, lines 16-19)
- confidential information (also column 1, lines 16-19)
- means for varying supply to the effective data processing portion (column 2, lines 41-46 and column 3, lines 36-44) in order to secure said confidential data (column 5, lines 34-37) against attacks based on current consumption (column 1, lines 40-45 and column 2, lines 29-46).

According to D1, it is the current that changes in a pseudo-random manner. Contrary to this, Claims 1 and 7 state that the supply voltage is modified. However, a person skilled in the art knows that a

variation in the voltage always involves (leads to) a variation in the corresponding current, and vice versa. The interdependence of the current and the voltage is well known to a person skilled in the art.

Document D2 also suggests the basic idea of the present application.

Claims 1 and 7 are therefore not inventive (PCT Article 33(3)).

3. The features of **Claims 2-6** are merely one of the options that a person skilled in the art could select, depending on the circumstances, from several obvious options in order to solve the stated problem without exercising an inventive step.

4. A feature that clearly defines the subdivision of the microcontroller into two parts, µC1 and µCE, and states that the supply voltage is modified (manipulated) for the µCE part only, is missing from the claims. This fundamental idea is not found in the prior art.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

It is not indicated in the description in relation to what document the claims are delimited (PCT Rule 6.3(b)).

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Although **Claims 1 and 7** have been drafted as separate independent claims, it appears that they have the same subject matter and that they differ only by virtue of a variation in the definition of the subject matter for which protection is sought and/or by virtue of the terms used to define the features. Therefore, said claims are not concise.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire 76.0591	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR00/02058	Date du dépot international *(jour/mois/année)* 17/07/2000	Date de priorité *(jour/mois/année)* 22/07/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06K19/073		
Déposant SCHLUMBERGER SYSTEMES et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 5 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

   - I ☒ Base du rapport
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☒ Irrégularités dans la demande internationale
   - VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
14/02/2001	07.09.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Heusler, N N° de téléphone +49 89 2399 2359

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/02058

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1,2,4,5,7-18	version initiale			
3,3a,6	reçue(s) le	16/07/2001	avec la lettre du	11/07/2001

Revendications, N°:

8-12	version initiale			
1-7	reçue(s) le	16/07/2001	avec la lettre du	11/07/2001

Dessins, feuilles:

1-8	version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

☐ de la description, pages :

☐ des revendications, n^{os} :

☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-7
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-7
Possibilité d'application industrielle	Oui :	Revendications	1-7
	Non :	Revendications	

2. Citations et explications
voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Il est fait référence aux documents suivants:

D1 = US - A - 4 932 053

D2 = US - A - 4 827 451

Concernant le point V

nouveauté, activité inventive; citations et explications (article 33 (2, 3) PCT; règle 66.2 a ii PCT)

1. La présente invention **concerne** un micro-contrôleur destiné à être incorporé, par exemple, dans une carte à puce. Le circuit intégré comporte deux parties actives: une partie micro-contrôleur interface (µCI dans la figure 5) et une partie efficace de traitement de données (µCE avec CPU, RAM, EEPROM, ROM etc.).

   Le **problème** que se propose de résoudre la présente invention peut être vue dans la sécurisation d'un tel micro-contrôleur contre des "attaques en courant" (attaque en vue d'obtenir des données confidentielles gérées par le micro-contrôleur, par exemple des clés, en visualisant le courant I_{cc} du micro-contrôleur en fonction du temps au moyen d'un ordinateur couplé, par exemple, à un oscilloscope numérique, pour échantillonner et numériser les résultats obtenus en vue d'une analyse en temps différé). Le **solution** proposée dans l'invention est un moyen pour faire varier la tension d'alimentation de la partie efficace de traitement de données (µCE) dite. Cette variation (de préférence, de manière aléatoire) de la tension bouleverse les signatures électriques et rend leur analyse difficile voire impossible. L'énergie consommée par le micro-contrôleur n'est donc pas révélatrice des instructions exécutées par le micro-contrôleur et par suite révélatrice des données confidentielles mises en jeu dans l'éxecution des dites instructions. Il n'est plus possible d'obtenir des informations confidentielles en analysant le courent I_{cc}.

2. Le **document** D1 se réfère au même problème que l'application (voir abstrait, col. 1, lignes 40-45 et col. 2, lignes 29-46). Cet art antérieur le plus proche décrit un micro-contrôleur destiné à être incorporé dans une carte à puce (col. 1, ligne 13), comprenant
   - un plot pour l'alimentation du dit micro-contrôleur (col. 3, ligne 29: V_{cc})
   - un plot d'entrée et de sortie de données (col. 1, ligne 22)
   - une partie efficace de traitement de données (col. 1, lignes 16-19)
   - des informations confidentielles (également col. 1, lignes 16-19)
   - des moyens pour faire varier l'alimentation de la partie efficace de traitement de données (col. 2, lignes 41-46 et col. 3, lignes 36-44) afin de sécuriser lesdites données confidentielles (col. 5, lignes 34-37) contre les attaques en courant (col. 1, lignes 40- 45 et col. 2, lignes 29-46).

Selon D1, c'est le courant qui change de manière pseudo aléatoire. Contrairement à ça, la revendication 1 et 7 définit que la tension d'alimentation est modifiée. Cependant un homme du métier sait que une variation de la tension implique (entraîne) toujours une variation du courant correspondante, et inversement. La dépendance entre le courant et la tension est bien connue à un homme du métier.

Aussi le document D2 suggère l'idée fondamentale de la présente application.

Les **revendications 1 et 7** ne sont donc pas inventives (art. 33 (3) PCT).

3. Les caractéristiques des **revendications 2-6** représentent seulement une des possibilités que la personne du métier pourrait choisir, selon le cas d'espèce, parmi plusieurs possibilités évidentes, pour résoudre le problème posé sans qu'une activité inventive soit impliquée.

4. Une caractéristique qui clairement définit la subdivision du microcontrôleur en deux parties µCI et µCE, et que la tension d'alimentation est modifiée (manipulée) pour la partie µCE seulement manque dans les revendications. Cette idée fondamentale ne se trouve pas dans l'art antérieur.

Concernant le point VII
Irrégularités dans la demande internationale (règles 5 - 7 PCT)

Il n'est pas indiqué dans la description par rapport à quel document les revendications ont été délimitées (règle 6.3 b PCT).

Concernant le point VIII
Observations: clarté, concision, support par la description (article 6 PCT)

Bien que les **revendications 1 et 7** aient été rédigées sous forme de revendications indépendantes distinctes, il semble qu'elles aient le même objet et qu'elles ne diffèrent l'une de l'autre que par une variation dans la définition de l'objet pour lequel la protection est demandée et/ou par les termes utilisés pour en définir les caractéristiques. Par conséquent ces revendications ne sont pas concises.

bruit ri[redacted]en informations aléatoires [redacted]erronées au cours de l'exécution des instructions par le micro-contrôleur.

Ces procédés montrent cependant de multiples inconvénients. Le temps d'exécution des programmes est long. L'espace mémoire qu'ils occupent est important. Enfin, les données confidentielles ne sont finalement pas protégées contre une analyse approfondie réalisée par les fraudeurs puisque la signature électrique, qui résulte de l'exécution des instructions, est toujours présente.

Un autre procédé, décrit dans la demande de brevet français enregistrée sous le numéro 98 01305, et non rendue publique à la date de priorité de la présente demande, propose de filtrer le courant par une cellule de filtrage passe-bas. Ce procédé permet uniquement d'atténuer les signatures électriques et leur analyse précise permet en définitive d'accéder à certaines données confidentielles.

Le brevet US 4 932 053 concerne quant à lui, la sécurité d'informations confidentielles contenues dans un circuit intégré. Dans un certain nombre d'applications concernant des circuits intégrés et plus particulièrement dans des applications du type carte à puce, il est nécessaire d'interdire l'accès de certaines données confidentielles contenues dans la mémoire du circuit à des personnes non autorisées. Afin d'empêcher le fraudeur de procéder à un examen de la consommation en courant aux extrémités du circuit intégré lors d'une opération de lecture ou d'écriture dans la mémoire, un circuit de protection est utilisé. Ce circuit de protection permet d'activer la simulation, selon une séquence pseudo-aléatoire générée par un générateur, de valeurs de consommation en courant identiques à celles des cellules mémoires réelles.

Notons enfin que le brevet US 4 827451 concerne le domaine des mémoires construites sous forme d'une matrice de cellules mémoires. Lesdites cellules, étant accessibles par les lignes et les colonnes , sont connectées à des circuits de lecture et d'écriture qui sont utilisés pour les programmer selon deux états - "1" ou "0" selon les données d'entrées – et lire l'état ainsi programmé. Les cellules mémoires sont du type nécessitant un courant de programmation afin d'être programmées à "1" et ne nécessitant aucun courant lors de la programmation à "0". Ledit circuit de sécurité consiste en un circuit de simulation s'activant lors d'une programmation à "0" pour délivrer un courant identique à celui délivré par une cellule mémoire lors d'une programmation à "1".

Compte tenu de ce qui précède, un problème technique que se propose de résoudre l'invention est de sécuriser un objet portatif du type carte à puce, comprenant :

- un micro-contrôleur comprenant une partie efficace pour effectuer un traitement de données;
- un plot pour l'alimentation en courant dudit micro-contrôleur ;
- un plot d'entrée et/ou de sortie de données ;
- des données confidentielles,

contre des attaques en courant.

A cette fin l'invention propose un objet portatif défini selon la revendication 1, ainsi qu'un micro-contrôleur défini selon la revendication 7.

micro-contrôleur selon l'état de la technique (signature A) puis dans le cas d'un micro-contrôleur sécurisé selon l'invention (signature B) ;

- la figure 12 est un schéma électrique d'un mode de réalisation particulier d'un micro-contrôleur selon l'invention ; et
- la figure 13 montre les variations des signaux S_1, S_2 et S_3 en fonction du temps, dans le cas d'un micro-contrôleur correspondant au mode de réalisation de la figure 12.

Dans le mode de réalisation montré aux figures 1, 2 et 3, un objet portatif selon l'invention se présente sous la forme d'une carte 1 sensiblement parallélépipèdique rectangle et de faible épaisseur dont un corps 2 intègre un module 3 électronique.

Le corps 2 de carte est par exemple constitué de cinq feuilles 20, 21, 22, 23 et 24 plastiques laminées et comporte une cavité 25 pour l'incorporation du module 3.

Le module 3 comprend un micro-contrôleur 30 dont des plots 300 de contact sont connectés électriquement, au moyen de fils 31 conducteurs, à des plages 32 de contact affleurantes à la surface du corps 2 de carte. Ces plages 32 reposent sur une épaisseur 33 d'un diélectrique du type verre époxy. L'ensemble micro-contrôleur 30 et fils 31 conducteurs est enrobé dans une résine 34 protectrice.

Dans le mode de réalisation de la figure 4, le micro-contrôleur 30 se présente sous la forme d'un parallélépipède rectangle dont l'épaisseur est de l'ordre de 180 µm et dont la surface est de l'ordre de 10 mm^2.

Ce micro-contrôleur 30 comporte une couche principale 301 de silicium dont la face active, qui intègre un circuit et porte les plots 300

REVENDICATIONS

1. Objet portatif (1) du type carte à puce, comprenant :

- un micro-contrôleur (30) comprenant une partie efficace (µCE) pour effectuer un traitement de données ;
- un plot de contact (VCC) pour l'alimentation en courant dudit micro-contrôleur (30) ;
- un plot (I/O) d'entrée et/ou de sortie de données ;
- des informations confidentielles ;

caractérisé en ce que l'objet portatif comprend en outre :

- un circuit interface (GEN, CAP, COM) à travers lequel la partie efficace (µCE) reçoit une tension d'alimentation (VµCE), ledit circuit interface (GEN, CAP, COM) étant agencé pour faire varier la tension d'alimentation de la partie efficace de traitement de données (µCE) afin de sécuriser lesdites données confidentielles contre les attaques en courant.

2. Objet portatif du type carte à puce selon la revendication 1 caractérisé en ce que le circuit d'interface comprend :

- un commutateur (COM) entre ledit plot de contact (VCC) et une borne d'alimentation de la partie efficace de traitement de données (µCE) ;
- une capacité (CAP) connectée entre ladite borne d'alimentation de la partie efficace du micro-contrôleur (µCE) et une autre borne d'alimentation de la partie efficace (µCE).

3 . Objet portatif du type carte à puce selon la revendication 2 caractérisé en ce que le circuit d'interface comprend un générateur d'impulsion (GEN) pour contrôler le commutateur (COM) de façon désynchronisée par rapport audit traîtement de données.

4. Objet portatif du type carte à puce selon la revendication 2 ou la revendication 3 caractérisé en ce que la capacité a une capacité supérieure à 1 nanofarad.

5. Objet portatif du type carte à puce selon la revendication 1 caractérisé en ce que le micro-contrôleur comporte une couche principale (301) de silicium dont la face active, qui intègre un circuit et porte les plots (300) de contact, est scellée à une couche complémentaire (302) de protection au moyen d'une couche de scellement (303).

6. Objet portatif du type carte à puce selon la revendication 5 caractérisé en ce que ledit circuit d'interface (COM, GEN, CAP) est situé dans la couche complémentaire de protection (302).

7. Micro-contrôleur (30) destiné à être incorporé dans un objet portatif (1) du type carte à puce comprenant :

- un plot de contact (VCC) pour l'alimentation en courant dudit micro-contrôleur (30);
- un plot (I/O) d'entrée et/ou de sortie de données ;
- une partie efficace (µCE) pour effectuer un traitement de données ;
- des informations confidentielles ;

caractérisé en ce qu'un circuit d'interface (COM, GEN, CAP) à travers lequel la partie efficace (µCE) reçoit une tension d'alimentation (VµCE), ledit circuit interface (COM, GEN, CAP) étant agencé pour faire varier la tension d'alimentation de la partie efficace de traitement de données (µCE) afin de sécuriser lesdites données confidentielles contre les attaques en courant.